CLAIMS:

1. A computer-readable medium having computer-executable instructions that, when executed by a computer, performs a method comprising:

obtaining a message M having two portions, wherein M_1 is one of the portions of the M and M_2 is another;

generating one or more codes having a combination with M_2 implicitly embedded therein, wherein calculations that generate the one or more codes do not employ M_2;

reporting the one or more codes.

2. A medium as recited in claim 1, wherein the method further comprises producing a digital signature (*DS*) comprising M_1 and the reported one or more codes.

3. A medium as recited in claim 1, wherein two or more codes are generated by the generating and reported by the reporting.

4. A medium as recited in claim 3, wherein a mathematical function for calculating one code is not identical to a mathematical function for calculating another code.

5. A medium as recited in claim 3, wherein the message M has a defined length and a length of a combination of two or more codes is less than the message's defined length.

6. A medium as recited in claim 3, wherein M_2 has a defined length and a length of a combination of two or more codes is less than or equal to the defined length of M_2.

7. A medium as recited in claim 1, wherein the generating comprises:

finding a value of a variable per-message key (k) where a predefined mathematical function employing k produces a result equivalent to M_2;

when such a value of k is found, calculating the two or more codes, where the calculation of one code is not identical to the calculation of any other code and where each calculation incorporates k.

8. A medium as recited in claim 1, wherein the generating comprises:

finding a value of a variable per-message key (k) where a predefined mathematical function employing k produces a result equivalent to M_2;

when such a value of k is found, calculating the two or more codes, where the calculation of one code is not identical to the calculation of any other code, the calculation of at least one code employs non-linear mathematical function, namely a quadratic equation, and where each calculation incorporates k.

9. A medium as recited in claim 3, wherein the generating comprises:

finding a value of a variable per-message key (k) where a predefined mathematical function employing M_1 and g^k produces a result equivalent to M_2;

when such a value of k is found, calculating the two or more codes, where one code is r and another is s, with r being calculated using another predefined mathematical function employing M_1 and g^k, and with s being calculated using still another predefined mathematical function employing M_1 and g^k and r.

10. A medium as recited in claim 3, wherein the method further comprises producing a digital signature (DS) comprising M_1 and the reported codes r and s.

11. A computing device comprising:

an audio/visual output;

a medium as recited in claim 1.

12. A computer-readable medium having computer-executable instructions that, when executed by a computer, performs a method comprising:

obtaining a message M having two portions, wherein M_1 is one of the portions of the M and M_2 is another;

generating two or more codes having a combination with M_2 implicitly embedded therein, wherein calculations that generate the codes do not employ M_2, wherein the generating comprises:

- finding a value of a variable per-message key (k) where a predefined mathematical function employing M_1 and g^k produces a result equivalent to M_2;
- when such a value of k is found, calculating the two or more codes, where the calculation of one code is not identical to the calculation of any other code and where each calculation incorporates k;

reporting the two or more codes.

13. A medium as recited in claim 12, wherein the method further comprises producing a digital signature (*DS*) comprising M_1 and the reported two or more codes.

14. A medium as recited in claim 12, wherein the calculation of at least one code employs a non-linear mathematical function.

15. A medium as recited in claim 12, wherein the message M has a defined length and a length of a combination of two or more codes is less than the message's defined length.

16. A medium as recited in claim 12, wherein M_2 has a defined length and a length of a combination of two or more codes is less than or equal to the defined length of M_2.

17. A medium as recited in claim 12, wherein one calculated code is r and another is s, with r being calculated using another predefined mathematical function employing M_1 and g^k, and with s being calculated using still another predefined mathematical function employing M_1 and g^k and r.

18. A medium as recited in claim 17, wherein the predefined mathematical function for s is non-linear.

19. A medium as recited in claim 17, wherein the method further comprises producing a digital signature (DS) comprising M_1 and the reported codes r and s.

20. A computing device comprising:

an audio/visual output;

a medium as recited in claim 12.

21. A computer-readable medium having computer-executable instructions that, when executed by a computer, performs a method comprising:

obtaining a digital signature (*DS*) having at least three portions, M_1, r, and s;

using a first predefined mathematical function employing M_1, r, and s, calculating the value of gk;

determining whether a second predefined mathematical function employing M_1 and gk produces a value equivalent to r

indicating the result of such determining.

22. A medium as recited in claim 21, wherein the method further comprises:

using a third predefined mathematical function employing M_1 and gk, calculating the value of M_2;

responsive to production of a value equivalent to r of the determining, producing a message comprising M_1 and M_2.

23. A medium as recited in claim 21, wherein the first predefined mathematical function does not include the value of k, thus the value of k remains unknown after the calculating the value of gk.

24. A medium as recited in claim 21, wherein the digital signature (*DS*) has at least one other portion, *auth*, and the method further comprises:

determining whether a fourth predefined mathematical function employing a secret key and gk produces a value equivalent to *auth*;

indicating the result of such determining.

25. A computing device comprising:

an audio/visual output;

a medium as recited in claim 21.

26. A method for facilitating digital security, the method comprising:

obtaining a message M having two portions, wherein M_1 is one of the portions of the M and M_2 is another;

generating two or more codes having a combination with M_2 implicitly embedded therein, wherein calculations that generate the codes do not employ M_2, wherein the generating comprises:

- finding a value of a variable per-message key (k) where a predefined mathematical function employing M_1 and g^k produces a result equivalent to M_2;
- when such a value of k is found, calculating the two or more codes, where the calculation of one code is not identical to the calculation of any other code and where each calculation incorporates k;

reporting the two or more codes.

27. A method as recited in claim 26 further comprising producing a digital signature (DS) comprising M_1 and the reported two or more codes.

28. A digital signature (*DS*) produced by a method as recited in claim 27 and embodied on a computer-readable medium.

29. A digital signature (*DS*) produced by a method as recited in claim 27 and embodied as human-readable indicia on a human-readable medium.

30. A method as recited in claim 26, wherein the calculation of at least one code employs a non-linear mathematical function.

31. A method as recited in claim 26, wherein the message M has a defined length and a length of a combination of two or more codes is less than the message's defined length.

32. A method as recited in claim 26, wherein M_2 has a defined length and a length of a combination of two or more codes is less than or equal to the defined length of M_2.

33. A method as recited in claim 26, wherein one calculated code is r and another is s, with r being calculated using another predefined mathematical function employing M_1 and g^k, and with s being calculated using still another predefined mathematical function employing M_1 and g^k and r.

34. A method as recited in claim 33, wherein the predefined mathematical function for s is non-linear.

35. A method as recited in claim 33, wherein the predefined mathematical function for s is quadratic.

36. A method as recited in claim 26 further comprising producing a message comprising M_1 and the reported codes r and s.

37. A message produced by a method as recited in claim 36 and embodied on a computer-readable medium.

38. A message produced by a method as recited in claim 36 and embodied as human-readable indicia on a human-readable medium.

39. A method for facilitating digital security, the method comprising:

obtaining a digital signature (*DS*) having at least three portions, M_1, r, and s;

using a first predefined mathematical function employing M_1, r, and s, producing the value of gk;

determining whether a second predefined mathematical function employing M_1 and gk produces a value equivalent to r

indicating the result of such determining.

40. A method as recited in claim 39 further comprising:

using a third predefined mathematical function employing M_1 and *gk*, producing the value of M_2;

responding to production of a value equivalent to *r* of the determining, producing a message comprising M_1 and M_2.

41. A method as recited in claim 39, wherein the first predefined mathematical function does not reference the value of *k*, thus the value of *k* remains unknown after the calculating the value of *gk*.

42. A method as recited in claim 39, wherein the digital signature (*DS*) has at least one other portion, *auth*, and the method further comprising:

determining whether a fourth predefined mathematical function employing a secret key and *gk* produces a value equivalent to *auth*;

indicating the result of such determining.

43. A method as recited in claim 39, wherein the obtaining comprises receiving input comprising the digital signature (*DS*) from a manual input unit of a computing device.